PORTAL
USPTO

Subscribe (Full Service) Register (Limited Service, Free) Login

Search: ● The ACM Digital Library ○ The Guide

biometric, card, identification, authentication SEARCH

THE ACM DIGITAL LIBRARY

Feedback Report a problem Satisfaction survey

Terms used: **biometric chip**

Found **11,463** of **207,474**

Sort results by relevance

Display results expanded form

Save results to a Binder

Search Tips

□ Open results in a new window

Try an Advanced Search

Try this search in The ACM Guide

Results 1 - 20 of 200

Best 200 shown

Result page: **1** 2 3 4 5 6 7 8 9 10 next

Relevance scale □□■■■

1 Privacy made public: will national security be the end of individualism? ■

Jennifer M. Fujawa

March 2005 **ACM SIGCAS Computers and Society**, Volume 35 Issue 1

Publisher: ACM Press

Full text available: html(20.78 KB) Additional Information: full citation, references, index terms

2 Computer architecture: A 3.84 gbits/s AES crypto coprocessor with modes of operation in a 0.18-μm CMOS technology ■

Alireza Hodjat, David D. Hwang, Bocheng Lai, Kris Tiri, Ingrid Verbauwhede

April 2005 **Proceedings of the 15th ACM Great Lakes symposium on VLSI GLSVSLI '05**

Publisher: ACM Press

Full text available: pdf(283.76 KB) Additional Information: full citation, abstract, references, citings, index terms

In this paper an AES crypto coprocessor that is fabricated using a 0.18-μm CMOS technology is presented. This crypto coprocessor performs the AES-128 encryption in both feedback and non-feedback modes of operation. A maximum throughput of 3.84 Gbits/s is achieved at a 330 MHz clock frequency for ECB, OFB, and CBC modes of operation. This crypto coprocessor can be programmed using the memory-mapped interface of an embedded CPU core and is tested using a LEON 32-bit (SPARC V8) processor in th ...

Keywords: ASIC, FPGA, VLSI, advanced encryption standard (AES), crypto-processor, cryptography, hardware architectures, security

3 Risk transparency: Privacy and security threat analysis of the federal employee personal identity verification (PIV) program ■

Paul A. Karger

July 2006 **Proceedings of the second symposium on Usable privacy and security SOUPS '06**

Publisher: ACM Press

Full text available: pdf(113.11 KB) Additional Information: full citation, abstract, references, index terms

This paper is a security and privacy threat analysis of new Federal Information Processing Standard for Personal Identity Verification (FIPS PUB 201). It identifies some problems with the standard, and it proposes solutions to those problems, using standardized cryptographic techniques that are based on the Internet Key Exchange (IKE) protocol [16]. When the standard is viewed in the abstract, it seems to effectively provide security and privacy, because it uses strong cryptographic algorithms. ...

Keywords: personal identification, privacy, smart cards

4 Student papers: The other side of identity theft: not just a financial concern
Kim Luong
September 2006 **Proceedings of the 3rd annual conference on Information security curriculum development InfoSecCD '06**
Publisher: ACM Press
Full text available: pdf(38.11 KB) Additional Information: full citation, abstract, references, index terms

With identity theft on the rise and the past history of legislation pertaining to it, it is important to look at recent updates and efforts to battle and handle this threat to society. Society needs to understand all realms of identity theft, how they occur, the protections and the rights they hold, and what their options are should they fall victim to this wave of crime. This paper looks at all of these issues and specifically focuses on the area of criminal record identity theft versus the ...

Keywords: identity theft, information security

5 Probabilistic quorum protocols for biometrical user authentication in OLTP
V. K. Murthy
January 1996 **ACM SIGSAC Review**, Volume 14 Issue 1
Publisher: ACM Press
Full text available: pdf(398.59 KB) Additional Information: full citation, abstract, references, citings

A statistical zero-knowledge authentication scheme is described for security control in on-line database transaction processing systems (OLTP). This scheme uses probabilistic quorum protocols to validate users using their biometrical characteristics (such as speech, handwriting and keyboard characteristics). This authentication scheme can be implemented using the present-day smart card technology.

6 Voice biometrics
Judith A. Markowitz
September 2000 **Communications of the ACM**, Volume 43 Issue 9
Publisher: ACM Press
Full text available: pdf(240.49 KB) html(36.88 KB) Additional Information: full citation, references, citings, index terms

7 A fuzzy commitment scheme
Ari Juels, Martin Wattenberg
November 1999 **Proceedings of the 6th ACM conference on Computer and communications security CCS '99**
Publisher: ACM Press
Full text available: pdf(966.08 KB) Additional Information: full citation, abstract, references, citings, index terms

We combine well-known techniques from the areas of error-correcting codes and cryptography to achieve a new type of cryptographic primitive that we refer to as a fuzzy commitment scheme. Like a conventional cryptographic commitment scheme, our fuzzy commitment scheme is both concealing and binding: it is infeasible for an attacker to learn the committed value, and also for the committer to decommit a value in more than one way. In a convent ...

8 Risks to the public: Risks to the public
Peter G. Neumann
January 2006 **ACM SIGSOFT Software Engineering Notes**, Volume 31 Issue 1
Publisher: ACM Press
Full text available: pdf(139.10 KB) Additional Information: full citation, abstract, index terms

Edited by Peter G. Neumann (Risks Forum Moderator and Chairman of the ACM Committee on Computers and Public Policy), plus personal contributions by others, as indicated. Opinions expressed are individual rather than organizational, and all of the usual disclaimers apply. We address problems relating to software, hardware, people, and other circumstances relating to computer systems. To economize on space, we include pointers to items in the online Risks Forum: (R i j) denotes RISKS vol i number ...

9 Designing an alternative for IS 2002.4 Information Technology Hardware and Systems Software course for an information assurance program
Felix F. Dreher
October 2005 **Journal of Computing Sciences in Colleges**, Volume 21 Issue 1
Publisher: Consortium for Computing Sciences in Colleges
Full text available: pdf(181.49 KB) Additional Information: full citation, abstract, references, index terms

While there are several well-known model curricula for Information System programs, there is great diversity in such programs as faculty design programs to address student backgrounds, careers choices, and the culture of the academic unit. Faculty interests and computer resources available to support the program will also influence the content of the curriculum and courses. Recently, programs have emerged that address the need to protect information resources stored in networked computer systems ...

10 Columns: Risks to the public in computers and related systems
Peter G. Neumann
November 2003 **ACM SIGSOFT Software Engineering Notes**, Volume 28 Issue 6
Publisher: ACM Press
Full text available: pdf(124.63 KB) Additional Information: full citation

11 A smartcard for authentication in WLANs
Marc Loutrel, Pascal Urien, Guy Pujolle
October 2003 **Proceedings of the 2003 IFIP/ACM Latin America conference on Towards a Latin American agenda for network research LANC '03**
Publisher: ACM Press
Full text available: pdf(333.05 KB) Additional Information: full citation, abstract, references, index terms

Wireless LANs based on the IEEE 802.11b standard have spread very quickly over the past few years. Nevertheless a lot of security issues remain and stop its deployment in corporations. One of the most important issues is the authentication of a terminal to an Access Point. We propose an interface to integrate the Extensible Authentication Protocol into smartcards and will show that smartcards could constitute the de-facto device for authentication in Wireless LAN as they are for GSM and will ...

Keywords: authentication, smartcard, wireless LANs

12 Playful interactions in PD: Make it so! Jean-Luc Picard, Bart Simpson and the design

of e-public services
Andy Dearden, Angela Lauener, Frances Slack, Chris Roast, Steve Cassidy
August 2006 **Proceedings of the ninth conference on Participatory design: Expanding boundaries in design - Volume 1 PDC '06**
Publisher: ACM Press
Full text available: pdf(100.94 KB) Additional Information: full citation, abstract, references, index terms

In this paper, we report on a project applying participatory design methods to include people who have experience of social exclusion (in one form or another) in designing possible technologies for e-(local)-government services. The work was part of a project for the Office of the Deputy Prime Minister in the UK, and was concerned with 'access tokens' that can provide personal identification for individuals accessing public services, based on technologies such as multi-functional smartcards, fla ...

Keywords: DATES project, e-government, pastiche scenarios, smartcards

13 IFIP
B. C. Glasson
June 1998 **ACM SIGMIS Database**, Volume 29 Issue 3
Publisher: ACM Press
Full text available: pdf(227.45 KB) Additional Information: full citation, index terms

14 Summary of the sixth SIGOPS European workshop on “matching operating systems to application needs”
Marc Shapiro
January 1995 **ACM SIGOPS Operating Systems Review**, Volume 29 Issue 1
Publisher: ACM Press
Full text available: pdf(441.58 KB) Additional Information: full citation, index terms

15 Architectures for cryptography and security applications: A side-channel leakage free coprocessor IC in 0.18μm CMOS for embedded AES-based cryptographic and biometric processing
K. Tiri, D. Hwang, A. Hodjat, B. Lai, S. Yang, P. Schaumont, I. Verbauwhede
June 2005 **Proceedings of the 42nd annual conference on Design automation DAC '05**
Publisher: ACM Press
Full text available: pdf(2.92 MB) Additional Information: full citation, abstract, references, citings, index terms

Security ICs are vulnerable to side-channel attacks (SCAs) that find the secret key by monitoring the power consumption and other information that is leaked by the switching behavior of digital CMOS gates. This paper describes a side-channel attack resistant coprocessor IC and its design techniques. The IC has been fabricated in 0.18μm CMOS. The coprocessor, which is used for embedded cryptographic and biometric processing, consists of four components: an Advanced Encryption Standard (AES) ...

Keywords: countermeasure, differential power analysis, encryption, security IC, side-channel attack, smart card

16 Oral II: New pen device for biometrical 3D pressure analysis of handwritten characters, words and signatures

Christian Hook, Juergen Kempf, Georg Scharfenberg
November 2003 **Proceedings of the 2003 ACM SIGMM workshop on Biometrics methods and applications WBMA '03**
Publisher: ACM Press
Full text available: pdf(593.61 KB) Additional Information: full citation, abstract, references, index terms

The demand for biometric applications in security, human computer interaction and related areas is rapidly increasing. This paper presents an unique biometrical smart pen BiSP for personal identification and handwriting recognition that has been developed in our laboratory. The system is superior to many other biometric techniques which have considerable disadvantages in practice. Several ballpoint like prototypes based on integrated sensors have been designed and constructed. In this report we ...

Keywords: acoustic handwriting recognition, biometric identification, microphone pen, multimodal biometrics, pen-pressure analysis, signature verification

17 BITS: a smartcard protected operating system
Paul C. Clark, Lance J. Hoffman
November 1994 **Communications of the ACM**, Volume 37 Issue 11
Publisher: ACM Press
Full text available: pdf(3.80 MB) Additional Information: full citation, references, citings, index terms

18 Towards design and validation of mixed-technology SOCs
S. Mir, B. Charlot, G. Nicolescu, P. Coste, F. Parrain, N. Zergainoh, B. Courtois, A. Jerraya, M. Rencz
March 2000 **Proceedings of the 10th Great Lakes symposium on VLSI GLSVLSI '00**
Publisher: ACM Press
Full text available: pdf(581.54 KB) Additional Information: full citation, abstract, references, index terms

This paper illustrates an approach to design and validation of heterogeneous systems. The emphasis is placed on devices which incorporate MEMS parts in either a single mixed-technology (CMOS + micromachining) SOC device, or alternatively as a hybrid system with the MEMS part in a separate chip. The design flow is general, and it is illustrated for the case of applications embedding CMOS sensors. In particular, applications based on finger-print recognition are considered since a ric ...

***Keywords**: HDLs, MEMS, SOCs, architecture exploration, cosimulation, design, verification*

19 Staying connected: Let your fingers do the talking
Meg McGinity
January 2005 **Communications of the ACM**, Volume 48 Issue 1
Publisher: ACM Press
Full text available: pdf(63.56 KB) html(14.42 KB) Additional Information: full citation, abstract, index terms

Biometrics is pointing its way into everyday applications. But figuring out how it fits into telecom and wireless services, never mind society, might just get downright touchy.

20 Microarchitecture-level power analysis and optimization techniques: Cooperative multithreading on 3mbedded multiprocessor architectures enables energy-scalable design

Patrick Schaumont, Bo-Cheng Charles Lai, Wei Qin, Ingrid Verbauwhede
June 2005 **Proceedings of the 42nd annual conference on Design automation DAC '05**
Publisher: ACM Press

Full text available: pdf(952.12 KB) Additional Information: full citation, abstract, references, citings, index terms

We propose an embedded multiprocessor architecture and its associated thread-based programming model. Using a cycle-true simulation model of this architecture, we are able to estimate energy savings for a threaded C program. The savings are obtained by voltage- and frequency-scaling of the individual processors. We port a fingerprint minutiae detection application onto this architecture, and show the resulting performance on single-, dual-, and quad-processor configurations. The energy-scaled qu ...

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next

PORTAL
USPTO

Subscribe (Full Service) Register (Limited Service, Free) Login

Search: ● The ACM Digital Library ○ The Guide

biometric, chip SEARCH

THE ACM DIGITAL LIBRARY

Feedback Report a problem Satisfaction survey

Terms used: **biometric chip**

Found **11,463** of **207,474**

Sort results by: relevance

Display results: expanded form

Save results to a Binder

Search Tips

□ Open results in a new window

Try an Advanced Search

Try this search in The ACM Guide

Results 1 - 20 of 200

Result page: **1** 2 3 4 5 6 7 8 9 10 next

Best 200 shown

Relevance scale

1 Privacy made public: will national security be the end of individualism?

Jennifer M. Fujawa

March 2005 **ACM SIGCAS Computers and Society**, Volume 35 Issue 1

Publisher: ACM Press

Full text available: html(20.78 KB) Additional Information: full citation, references, index terms

2 Computer architecture: A 3.84 gbits/s AES crypto coprocessor with modes of operation in a 0.18-μm CMOS technology

Alireza Hodjat, David D. Hwang, Bocheng Lai, Kris Tiri, Ingrid Verbauwhede

April 2005 **Proceedings of the 15th ACM Great Lakes symposium on VLSI GLSVSLI '05**

Publisher: ACM Press

Full text available: pdf(283.76 KB) Additional Information: full citation, abstract, references, citings, index terms

In this paper an AES crypto coprocessor that is fabricated using a 0.18-μm CMOS technology is presented. This crypto coprocessor performs the AES-128 encryption in both feedback and non-feedback modes of operation. A maximum throughput of 3.84 Gbits/s is achieved at a 330 MHz clock frequency for ECB, OFB, and CBC modes of operation. This crypto coprocessor can be programmed using the memory-mapped interface of an embedded CPU core and is tested using a LEON 32-bit (SPARC V8) processor in th ...

Keywords: ASIC, FPGA, VLSI, advanced encryption standard (AES), crypto-processor, cryptography, hardware architectures, security

3 Risk transparency: Privacy and security threat analysis of the federal employee personal identity verification (PIV) program

Paul A. Karger

July 2006 **Proceedings of the second symposium on Usable privacy and security SOUPS '06**

Publisher: ACM Press

Full text available: pdf(113.11 KB) Additional Information: full citation, abstract, references, index terms

This paper is a security and privacy threat analysis of new Federal Information Processing Standard for Personal Identity Verification (FIPS PUB 201). It identifies some problems with the standard, and it proposes solutions to those problems, using standardized cryptographic techniques that are based on the Internet Key Exchange (IKE) protocol [16]. When the standard is viewed in the abstract, it seems to effectively provide security and privacy, because it uses strong cryptographic algorithms. ...

Keywords: personal identification, privacy, smart cards

4 Student papers: The other side of identity theft: not just a financial concern
Kim Luong
September 2006 **Proceedings of the 3rd annual conference on Information security curriculum development InfoSecCD '06**
Publisher: ACM Press
Full text available: pdf(38.11 KB) Additional Information: full citation, abstract, references, index terms

With identity theft on the rise and the past history of legislation pertaining to it, it is important to look at recent updates and efforts to battle and handle this threat to society. Society needs to understand all realms of identity theft, how they occur, the protections and the rights they hold, and what their options are should they fall victim to this wave of crime. This paper looks at all of these issues and specifically focuses on the area of criminal record identity theft versus the ...

Keywords: identity theft, information security

5 Probabilistic quorum protocols for biometrical user authentication in OLTP
V. K. Murthy
January 1996 **ACM SIGSAC Review**, Volume 14 Issue 1
Publisher: ACM Press
Full text available: pdf(398.59 KB) Additional Information: full citation, abstract, references, citings

A statistical zero-knowledge authentication scheme is described for security control in on-line database transaction processing systems (OLTP). This scheme uses probabilistic quorum protocols to validate users using their biometrical characteristics (such as speech, handwriting and keyboard characteristics). This authentication scheme can be implemented using the present-day smart card technology.

6 Voice biometrics
Judith A. Markowitz
September 2000 **Communications of the ACM**, Volume 43 Issue 9
Publisher: ACM Press
Full text available: pdf(240.49 KB)
html(36.88 KB) Additional Information: full citation, references, citings, index terms

7 A fuzzy commitment scheme
Ari Juels, Martin Wattenberg
November 1999 **Proceedings of the 6th ACM conference on Computer and communications security CCS '99**
Publisher: ACM Press
Full text available: pdf(966.08 KB) Additional Information: full citation, abstract, references, citings, index terms

We combine well-known techniques from the areas of error-correcting codes and cryptography to achieve a new type of cryptographic primitive that we refer to as a fuzzy commitment scheme. Like a conventional cryptographic commitment scheme, our fuzzy commitment scheme is both concealing and binding: it is infeasible for an attacker to learn the committed value, and also for the committer to decommit a value in more than one way. In a convent ...

8 Risks to the public: Risks to the public
Peter G. Neumann
January 2006 **ACM SIGSOFT Software Engineering Notes**, Volume 31 Issue 1
Publisher: ACM Press
Full text available: pdf(139.10 KB) Additional Information: full citation, abstract, index terms

Edited by Peter G. Neumann (Risks Forum Moderator and Chairman of the ACM Committee on Computers and Public Policy), plus personal contributions by others, as indicated. Opinions expressed are individual rather than organizational, and all of the usual disclaimers apply. We address problems relating to software, hardware, people, and other circumstances relating to computer systems. To economize on space, we include pointers to items in the online Risks Forum: (R i j) denotes RISKS vol i number ...

9 Designing an alternative for IS 2002.4 Information Technology Hardware and Systems Software course for an information assurance program
Felix F. Dreher
October 2005 **Journal of Computing Sciences in Colleges**, Volume 21 Issue 1
Publisher: Consortium for Computing Sciences in Colleges
Full text available: pdf(181.49 KB) Additional Information: full citation, abstract, references, index terms

While there are several well-known model curricula for Information System programs, there is great diversity in such programs as faculty design programs to address student backgrounds, careers choices, and the culture of the academic unit. Faculty interests and computer resources available to support the program will also influence the content of the curriculum and courses. Recently, programs have emerged that address the need to protect information resources stored in networked computer systems ...

10 Columns: Risks to the public in computers and related systems
Peter G. Neumann
November 2003 **ACM SIGSOFT Software Engineering Notes**, Volume 28 Issue 6
Publisher: ACM Press
Full text available: pdf(124.63 KB) Additional Information: full citation

11 A smartcard for authentication in WLANs
Marc Loutrel, Pascal Urien, Guy Pujolle
October 2003 **Proceedings of the 2003 IFIP/ACM Latin America conference on Towards a Latin American agenda for network research LANC '03**
Publisher: ACM Press
Full text available: pdf(333.05 KB) Additional Information: full citation, abstract, references, index terms

Wireless LANs based on the IEEE 802.11b standard have spread very quickly over the past few years. Nevertheless a lot of security issues remain and stop its deployment in corporations. One of the most important issues is the authentication of a terminal to an Access Point. We propose an interface to integrate the Extensible Authentication Protocol into smartcards and will show that smartcards could constitute the de-facto device for authentication in Wireless LAN as they are for GSM and will ...

Keywords: authentication, smartcard, wireless LANs

12 Playful interactions in PD: Make it so! Jean-Luc Picard, Bart Simpson and the design

of e-public services
Andy Dearden, Angela Lauener, Frances Slack, Chris Roast, Steve Cassidy
August 2006 **Proceedings of the ninth conference on Participatory design: Expanding boundaries in design - Volume 1 PDC '06**
Publisher: ACM Press
Full text available: pdf(100.94 KB) Additional Information: full citation, abstract, references, index terms

In this paper, we report on a project applying participatory design methods to include people who have experience of social exclusion (in one form or another) in designing possible technologies for e-(local)-government services. The work was part of a project for the Office of the Deputy Prime Minister in the UK, and was concerned with 'access tokens' that can provide personal identification for individuals accessing public services, based on technologies such as multi-functional smartcards, fla ...

Keywords: DATES project, e-government, pastiche scenarios, smartcards

13 IFIP
B. C. Glasson
June 1998 **ACM SIGMIS Database**, Volume 29 Issue 3
Publisher: ACM Press
Full text available: pdf(227.45 KB) Additional Information: full citation, index terms

14 Summary of the sixth SIGOPS European workshop on "matching operating systems to application needs"
Marc Shapiro
January 1995 **ACM SIGOPS Operating Systems Review**, Volume 29 Issue 1
Publisher: ACM Press
Full text available: pdf(441.58 KB) Additional Information: full citation, index terms

15 Architectures for cryptography and security applications: A side-channel leakage free coprocessor IC in 0.18μm CMOS for embedded AES-based cryptographic and biometric processing
K. Tiri, D. Hwang, A. Hodjat, B. Lai, S. Yang, P. Schaumont, I. Verbauwhede
June 2005 **Proceedings of the 42nd annual conference on Design automation DAC '05**
Publisher: ACM Press
Full text available: pdf(2.92 MB) Additional Information: full citation, abstract, references, citings, index terms

Security ICs are vulnerable to side-channel attacks (SCAs) that find the secret key by monitoring the power consumption and other information that is leaked by the switching behavior of digital CMOS gates. This paper describes a side-channel attack resistant coprocessor IC and its design techniques. The IC has been fabricated in 0.18μm CMOS. The coprocessor, which is used for embedded cryptographic and biometric processing, consists of four components: an Advanced Encryption Standard (AES) ...

Keywords: countermeasure, differential power analysis, encryption, security IC, side-channel attack, smart card

16 Oral II: New pen device for biometrical 3D pressure analysis of handwritten characters, words and signatures

Christian Hook, Juergen Kempf, Georg Scharfenberg
November 2003 **Proceedings of the 2003 ACM SIGMM workshop on Biometrics methods and applications WBMA '03**
Publisher: ACM Press
Full text available: pdf(593.61 KB) Additional Information: full citation, abstract, references, index terms

The demand for biometric applications in security, human computer interaction and related areas is rapidly increasing. This paper presents an unique biometrical smart pen BiSP for personal identification and handwriting recognition that has been developed in our laboratory. The system is superior to many other biometric techniques which have considerable disadvantages in practice. Several ballpoint like prototypes based on integrated sensors have been designed and constructed. In this report we ...

Keywords: acoustic handwriting recognition, biometric identification, microphone pen, multimodal biometrics, pen-pressure analysis, signature verification

17 BITS: a smartcard protected operating system
Paul C. Clark, Lance J. Hoffman
November 1994 **Communications of the ACM**, Volume 37 Issue 11
Publisher: ACM Press
Full text available: pdf(3.80 MB) Additional Information: full citation, references, citings, index terms

18 Towards design and validation of mixed-technology SOCs
S. Mir, B. Charlot, G. Nicolescu, P. Coste, F. Parrain, N. Zergainoh, B. Courtois, A. Jerraya, M. Rencz
March 2000 **Proceedings of the 10th Great Lakes symposium on VLSI GLSVLSI '00**
Publisher: ACM Press
Full text available: pdf(581.54 KB) Additional Information: full citation, abstract, references, index terms

This paper illustrates an approach to design and validation of heterogeneous systems. The emphasis is placed on devices which incorporate MEMS parts in either a single mixed-technology (CMOS + micromachining) SOC device, or alternatively as a hybrid system with the MEMS part in a separate chip. The design flow is general, and it is illustrated for the case of applications embedding CMOS sensors. In particular, applications based on finger-print recognition are considered since a ric ...

***Keywords**: HDLs, MEMS, SOCs, architecture exploration, cosimulation, design, verification*

19 Staying connected: Let your fingers do the talking
Meg McGinity
January 2005 **Communications of the ACM**, Volume 48 Issue 1
Publisher: ACM Press
Full text available: pdf(63.56 KB)
html(14.42 KB) Additional Information: full citation, abstract, index terms

Biometrics is pointing its way into everyday applications. But figuring out how it fits into telecom and wireless services, never mind society, might just get downright touchy.

20 Microarchitecture-level power analysis and optimization techniques: Cooperative multithreading on 3mbedded multiprocessor architectures enables energy-scalable design

Patrick Schaumont, Bo-Cheng Charles Lai, Wei Qin, Ingrid Verbauwhede

June 2005 **Proceedings of the 42nd annual conference on Design automation DAC '05**
Publisher: ACM Press

Full text available: pdf(952.12 KB) Additional Information: full citation, abstract, references, citings, index terms

We propose an embedded multiprocessor architecture and its associated thread-based programming model. Using a cycle-true simulation model of this architecture, we are able to estimate energy savings for a threaded C program. The savings are obtained by voltage- and frequency-scaling of the individual processors. We port a fingerprint minutiae detection application onto this architecture, and show the resulting performance on single-, dual-, and quad-processor configurations. The energy-scaled qu ...

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next

PORTAL
USPTO

Subscribe (Full Service) Register (Limited Service, Free) Login

Search: ● The ACM Digital Library ○ The Guide

biometric, chip, hash SEARCH

THE ACM DIGITAL LIBRARY

Feedback Report a problem Satisfaction survey

Terms used: **biometric chip hash**

Found **2,179** of **207,474**

Sort results by: relevance

Display results: expanded form

Save results to a Binder

Search Tips

□ Open results in a new window

Try an Advanced Search

Try this search in The ACM Guide

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next

Best 200 shown

Relevance scale

1 A fuzzy commitment scheme

Ari Juels, Martin Wattenberg

November 1999 **Proceedings of the 6th ACM conference on Computer and communications security CCS '99**

Publisher: ACM Press

Full text available: pdf(966.08 KB) Additional Information: full citation, abstract, references, citings, index terms

We combine well-known techniques from the areas of error-correcting codes and cryptography to achieve a new type of cryptographic primitive that we refer to as a fuzzy commitment scheme. Like a conventional cryptographic commitment scheme, our fuzzy commitment scheme is both concealing and binding: it is infeasible for an attacker to learn the committed value, and also for the committer to decommit a value in more than one way. In a convent ...

2 Architecture for Protecting Critical Secrets in Microprocessors

Ruby B. Lee, Peter C. S. Kwan, John P. McGregor, Jeffrey Dwoskin, Zhenghong Wang

May 2005 **ACM SIGARCH Computer Architecture News , Proceedings of the 32nd annual international symposium on Computer Architecture ISCA '05**, Volume 33 Issue 2

Publisher: IEEE Computer Society, ACM Press

Full text available: pdf(143.62 KB) Additional Information: full citation, abstract, cited by, index terms

We propose "secret-protected (SP)" architecture to enable secure and convenient protection of critical secrets for a given user in an on-line environment. Keys are examples of critical secrets, and key protection and management is a fundamental problem ¿ often assumed but not solved ¿ underlying the use of cryptographic protection of sensitive files, messages, data and programs. SP-processors contain a minimalist set of architectural features that can be built into a general-purpose microprocess ...

3 SecCMP: a secure chip-multiprocessor architecture

Li Yang, Lu Peng

October 2006 **Proceedings of the 1st workshop on Architectural and system support for improving software dependability ASID '06**

Publisher: ACM Press

Full text available: pdf(419.78 KB) Additional Information: full citation, abstract, references, index terms

Security has been considered as an important issue in processor design. Most of the existing mechanisms address security and integrity issues caused by untrusted main memory in single-core systems. In this paper, we propose a secure Chip-Multiprocessor architecture (*SecCMP*) to handle security related problems such as key protection and core authentication in multi-core systems. Threshold secret sharing scheme is employed to protect critical keys because secret sharing is a distributed sec ...

Keywords: chip-multiprocessor, encryption, fault-tolerance, security

4 Secure systems: Energy and execution time analysis of a software-based trusted platform module

Najwa Aaraj, Anand Raghunathan, Srivaths Ravi, Niraj K. Jha

April 2007 **Proceedings of the conference on Design, automation and test in Europe DATE '07**

Publisher: ACM Press

Full text available: pdf(838.82 KB) Additional Information: full citation, abstract, references

Trusted platforms have been proposed as a promising approach to enhance the security of general-purpose computing systems. However, for many resource-constrained embedded systems, the size and cost overheads of a separate Trusted Platform Module (TPM) chip are not acceptable. One alternative is to use a software-based TPM (SW-TPM), which implements TPM functions using software that executes in a protected execution domain on the embedded processor itself. However, since many embedded systems ...

5 Security as a new dimension in embedded system design: Security as a new dimension in embedded system design

Srivaths Ravi, Paul Kocher, Ruby Lee, Gary McGraw, Anand Raghunathan

June 2004 **Proceedings of the 41st annual conference on Design automation DAC '04**

Publisher: ACM Press

Full text available: pdf(209.10 KB) Additional Information: full citation, abstract, references, citings, index terms

The growing number of instances of breaches in information security in the last few years has created a compelling case for efforts towards secure electronic systems. Embedded systems, which will be ubiquitously used to capture, store, manipulate, and access data of a sensitive nature, pose several unique and interesting security challenges. Security has been the subject of intensive research in the areas of cryptography, computing, and networking. However, despite these efforts, *security is ...*

***Keywords**: PDAs, architectures, battery life, cryptography, design, design methodologies, digital rights management, embedded systems, performance, security, security processing, security protocols, sensors, software attacks, tamper resistance, trusted computing, viruses*

6 Authentication and authorization: Silicon physical random functions

Blaise Gassend, Dwaine Clarke, Marten van Dijk, Srinivas Devadas

November 2002 **Proceedings of the 9th ACM conference on Computer and communications security CCS '02**

Publisher: ACM Press

Full text available: pdf(433.69 KB) Additional Information: full citation, abstract, references, citings, index terms

We introduce the notion of a Physical Random Function (PUF). We argue that a complex integrated circuit can be viewed as a silicon PUF and describe a technique to identify and authenticate individual integrated circuits (ICs).We describe several possible circuit realizations of different PUFs. These circuits have been implemented in commodity Field Programmable Gate Arrays (FPGAs). We present experiments which indicate that reliable authentication of individual FPGAs can be performed even in the ...

Keywords: identification, physical random function, physical security, smartcard, tamper resistance, unclonability

7 Architectures for cryptography and security applications: A side-channel leakage free coprocessor IC in 0.18μm CMOS for embedded AES-based cryptographic and biometric processing
K. Tiri, D. Hwang, A. Hodjat, B. Lai, S. Yang, P. Schaumont, I. Verbauwhede
June 2005 **Proceedings of the 42nd annual conference on Design automation DAC '05**
Publisher: ACM Press
Full text available: pdf(2.92 MB) Additional Information: full citation, abstract, references, citings, index terms

Security ICs are vulnerable to side-channel attacks (SCAs) that find the secret key by monitoring the power consumption and other information that is leaked by the switching behavior of digital CMOS gates. This paper describes a side-channel attack resistant coprocessor IC and its design techniques. The IC has been fabricated in 0.18μm CMOS. The coprocessor, which is used for embedded cryptographic and biometric processing, consists of four components: an Advanced Encryption Standard (AES) ...

Keywords: countermeasure, differential power analysis, encryption, security IC, side-channel attack, smart card

8 Authentication: Pass-thoughts: authenticating with our minds
Julie Thorpe, P. C. van Oorschot, Anil Somayaji
September 2005 **Proceedings of the 2005 workshop on New security paradigms NSPW '05**
Publisher: ACM Press
Full text available: pdf(3.94 MB) Additional Information: full citation, abstract, references

We present a novel idea for user authentication that we call *pass-thoughts*. Recent advances in Brain-Computer Interface (BCI) technology indicate that there is potential for a new type of human-computer interaction: a user transmitting thoughts directly to a computer. The goal of a pass-thought system would be to extract as much entropy as possible from a user's brain signals upon "transmitting" a thought. Provided that these brain signals can be recorded and processed in an accurate and ...

Keywords: authentication, passwords

9 Security in embedded systems: Design challenges
Srivaths Ravi, Anand Raghunathan, Paul Kocher, Sunil Hattangady
August 2004 **ACM Transactions on Embedded Computing Systems (TECS)**, Volume 3 Issue 3
Publisher: ACM Press
Full text available: pdf(3.67 MB) Additional Information: full citation, abstract, references, citings, index terms, review

Many modern electronic systems---including personal computers, PDAs, cell phones, network routers, smart cards, and networked sensors to name a few---need to access, store, manipulate, or communicate sensitive information, making security a serious concern in their design. Embedded systems, which account for a wide range of products from the electronics, semiconductor, telecommunications, and networking industries, face some of the most demanding security concerns---on the one hand, they are oft ...

Keywords: Embedded systems, architecture, authentication, battery life, cryptographic algorithms, decryption, encryption, hardware design, processing requirements, security, security attacks, security protocols, tamper resistance

10 On-line e-wallet system with decentralized credential keepers
Stig Frode Mjølsnes, Chunming Rong
February 2003 **Mobile Networks and Applications**, Volume 8 Issue 1
Publisher: Kluwer Academic Publishers
Full text available: pdf(240.23 KB) Additional Information: full citation, abstract, references, index terms

We propose a generalization of the architecture of an electronic wallet, as first developed in the seminal European research project CAFE. With this model you can leave most of the content of your electronic wallet at the security of your residential electronic keeper, while roaming with your favorite mobile terminals. Emerging mobile handsets with both short range Bluetooth and cellular GPRS communications provide a sufficient communication platform for this electronic wallet architecture. Howe ...

Keywords: digital credentials, e-wallet architecture, mobile commerce, payment protocols, privacy

11 Oral II: Secure smartcardbased fingerprint authentication
T. Charles Clancy, Negar Kiyavash, Dennis J. Lin
November 2003 **Proceedings of the 2003 ACM SIGMM workshop on Biometrics methods and applications WBMA '03**
Publisher: ACM Press
Full text available: pdf(452.50 KB) Additional Information: full citation, abstract, references, citings, index terms

In this paper, the fundamental insecurities hampering a scalable, wide-spread deployment of biometric authentication are examined, and a cryptosystem capable of using fingerprint data as its key is presented. For our application, we focus on situations where a private key stored on a smartcard is used for authentication in a networked environment, and we assume an attacker can launch o -line attacks against a stolen card.Juels and Sudan's *fuzzy vault* is used as a starting point for buildi ...

Keywords: authentication, biometrics, fingerprint, smartcard

12 Database sharing and privacy: GhostDB: querying visible and hidden data without leaks
Nicolas Anciaux, Mehdi Benzine, Luc Bouganim, Philippe Pucheral, Dennis Shasha
June 2007 **Proceedings of the 2007 ACM SIGMOD international conference on Management of data SIGMOD '07**
Publisher: ACM Press
Full text available: pdf(416.88 KB) Additional Information: full citation, abstract, references, index terms

Imagine that you have been entrusted with private data, such as corporate product information, sensitive government information, or symptom and treatment information about hospital patients. You may want to issue queries whose result will combine private and public data, but private data must not be revealed. GhostDB is an architecture and system to achieve this. You carry private data in a smart USB key (a large Flash persistent store combined with a tamper and snoop-resistant CPU and small ...

Keywords: privacy, secure device, storage model

13 [Invited Talks: Secure information sharing enabled by Trusted Computing and PEI models](#)
Ravi Sandhu, Kumar Ranganathan, Xinwen Zhang
March 2006 **Proceedings of the 2006 ACM Symposium on Information, computer and communications security ASIACCS '06**
Publisher: ACM Press
Full text available: pdf(210.37 KB) Additional Information: full citation, abstract, references, index terms

The central goal of secure information sharing is to "share but protect" where the motivation to "protect" is to safeguard the sensitive content from unauthorized disclosure (in contrast to protecting the content to avoid loss of revenue as in retail Digital Rights Management). This elusive goal has been a major driver for information security for over three decades. Recently, the need for secure information sharing has dramatically increased with the explosion of the Internet and the convergenc ...

Keywords: PEI models, access control, authorization, secure information sharing, security framework, trusted computing

14 BITS: a smartcard protected operating system
Paul C. Clark, Lance J. Hoffman
November 1994 **Communications of the ACM**, Volume 37 Issue 11
Publisher: ACM Press
Full text available: pdf(3.80 MB) Additional Information: full citation, references, citings, index terms

15 Authentication/protocols: A secure biometric authentication scheme based on robust hashing
Yagiz Sutcu, Husrev Taha Sencar, Nasir Memon
August 2005 **Proceedings of the 7th workshop on Multimedia and security MM&Sec '05**
Publisher: ACM Press
Full text available: pdf(821.83 KB) Additional Information: full citation, abstract, references, index terms

In this paper, we propose a secure biometric based authentication scheme which fundamentally relies on the use of a robust hash function. The robust hash function is a one-way transformation tailored specifically for each user based on their biometrics. The function is designed as a sum of properly weighted and shifted Gaussian functions to ensure the security and privacy of biometric data. We discuss various design issues such as scalability, collision-freeness and security. We also provide tes ...

Keywords: authentication, biometrics, privacy, robust hashing, security

16 Embedded hardware design case studies: Design flow for HW / SW acceleration transparency in the thumbpod secure embedded system
David Hwang, Bo-Cheng Lai, Patrick Schaumont, Kazuo Sakiyama, Yi Fan, Shenglin Yang, Alireza Hodjat, Ingrid Verbauwhede
June 2003 **Proceedings of the 40th conference on Design automation DAC '03**
Publisher: ACM Press
Full text available: pdf(250.69 KB) Additional Information: full citation, abstract, references, index terms

This paper describes a case study and design flow of a secure embedded system called

ThumbPod, which uses cryptographic and biometric signal processing acceleration. It presents the concept of HW/SW acceleration transparency, a systematic method to accelerate Java functions in both software and hardware. An example of acceleration transparency for a Rijndael encryption function is presented. The embedded prototype hardware platform is also described. Acceleration transparency yields software and ...

17 Identification control: Owner-controlled information
Carrie Gates, Jacob Slonim
August 2003 **Proceedings of the 2003 workshop on New security paradigms NSPW '03**
Publisher: ACM Press
Full text available: pdf(1.06 MB) Additional Information: full citation, abstract, references

Information about individuals is currently maintained in many thousands of databases, with much of that information, such as name and address, replicated across multiple databases. However, this proliferation of personal information raises issues of privacy for the individual, as well as maintenance issues in terms of the accuracy of the information. Ideally, each individual would own, maintain and control his personal information, allowing access to those who needed at the time it was needed. O ...

Keywords: architecture, privacy, security

18 An interactive codesign environment for domain-specific coprocessors
Patrick Schaumont, Doris Ching, Ingrid Verbauwhede
January 2006 **ACM Transactions on Design Automation of Electronic Systems (TODAES)**, Volume 11 Issue 1
Publisher: ACM Press
Full text available: pdf(406.61 KB) Additional Information: full citation, abstract, references, citings, index terms

Energy-efficient embedded systems rely on domain-specific coprocessors for dedicated tasks such as baseband processing, video coding, or encryption. We present a language and design environment called GEZEL that can be used for the design, verification and implementation of such coprocessor-based systems.The GEZEL environment creates a platform simulator by combining a hardware simulation kernel with one or more instruction-set simulators. The hardware part of the platform is programmed in GEZEL ...

Keywords: Cosimulation, hardware description language, hardware-software codesign

19 Ubiquitous computing (UC): Extending the EPC network: the potential of RFID in anti-counterfeiting
Thorsten Staake, Frédéric Thiesse, Elgar Fleisch
March 2005 **Proceedings of the 2005 ACM symposium on Applied computing SAC '05**
Publisher: ACM Press
Full text available: pdf(106.51 KB) Additional Information: full citation, abstract, references, citings, index terms

The International Chamber of Commerce estimates that seven percent of the world trade is in counterfeit goods, with the counterfeit market being worth 500 billion USD in 2004. Many companies already use overt anti-counterfeiting measures like holograms to confine counterfeiting and product piracy. However, current techniques are not suited for automated tests of product authenticity as required in warehouses, or do not provide the required level of security. In this context, Radio Frequency Iden ...

Keywords: RFID, authentication, counterfeiting, track & trace

20 Computer forensics (CF): The advent of trusted computing: implications for digital forensics

Mike Burmester, Judie Mulholland
April 2006 **Proceedings of the 2006 ACM symposium on Applied computing SAC '06**
Publisher: ACM Press
Full text available: pdf(137.02 KB) Additional Information: full citation, abstract, references, index terms

The release of computer hardware devices based on "trusted computing" technologies is heralding a paradigm shift that will have profound implications for digital forensics. In this paper, we map out the contours of a trusted environment in order to establish the context for the paper. This is followed by the main components of the TC architecture with an emphasis on the Trusted Platform and the Trusted Platform Module (TPM). The next section presents a synopsis based on three threat models, *v* ...

Keywords: *cybercrime, data recovery, encryption, file systems, forensics, specifications, trusted computing*

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next

IEEE Xplore® RELEASE 2.3

Home | Login | Logout | Access Information | Alerts |

Welcome United States Patent and Trademark Office

□ Search Session History

BROWSE SEARCH IEEE XPLORE GUIDE

Edit an existing query or compose a new query in the Search Query Display.

Select a search number (#) to:

- Add a query to the Search Query Display
- Combine search queries using AND, OR, or NOT
- Delete a search
- Run a search

Sat, 21 Jul 2007, 4:50:04 PM EST

Search Query Display

[redacted] [redacted]

Recent Search Queries

#1	((biometric. chip)<in>metadata)
#2	(biometric, chip<IN>metadata)
#3	((biometric<in>metadata) <and> (chip<in>metadata))<and> (scanner<in>metadata)
#4	((biometric<in>metadata) <and> (chip<in>metadata))<and> (hash<in>metadata)
#5	((biometric<in>metadata) <and> (chip<in>metadata))<and> (hash<in>metadata)
#6	((biometric authentication<in>metadata) <and> (chip<in>metadata))
#7	((biometric<in>metadata) <and> (chip<in>metadata))<and> (~~smart card~~<in>metadata)
#8	((biometric<in>metadata) <and> (chip<in>metadata))<and> (~~smart card~~<in>metadata)

[redacted]

Help Contact Us Privacy &

Indexed by Inspec®